

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

UNITED STATES OF AMERICA,

Plaintiff,

v.

\$13,475,175.67 IN FUNDS SEIZED FROM  
MITSUBISHI UFJ TRUST AND BANKING  
CORPORATION ACCOUNT ENDING IN  
0328,

Defendant *in Rem*.

Civil No. 1:24-cv- 2333

**VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

COMES NOW the plaintiff, the United States of America, by and through its counsel, Jessica D. Aber, United States Attorney for the Eastern District of Virginia, Kevin Hudson, and Zoe Bedell, Assistant United States Attorneys, and brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

**NATURE OF THE ACTION**

1. The United States brings this action *in rem* seeking the forfeiture of all right, title, and interest in the defendant *in rem* identified in the case caption above (the “Defendant Property”).

2. The United States’ claim arises from an investment fraud scheme perpetrated against numerous individual victims. As described in more detail below, co-conspirators used social engineering to convince victims to “invest” in fraudulent cryptocurrency investment websites, which in fact funneled victim funds to those perpetrating the fraud, who then laundered those funds, frequently to a location outside the United States.

3. Specifically, the co-conspirators were directing victim monies to a number of U.S. bank accounts in the name of various shell companies. As relevant here, the shell company accounts would generally forward the victim monies in batches to a correspondent account held at Mitsubishi UFJ Trust and Banking Corporation (“MUFJ”) by Bank 1. From there, the funds were further forwarded to an account ending in 0328 held by Bank 2 at “MUFJ” in New York (“Subject Account”), and then forwarded to two bank accounts at Bank 2 in a location abroad.

4. This forwarding of funds from Bank 1 was done via “additional instructions” contained in each wire’s memo line, rather than by specifying the actual end destination of the funds. This method facilitated the co-conspirators’ fraud and money laundering schemes by evading scrutiny from Bank 1 and MUFJ and obscuring the source and destination of the funds. The wire forms initiating these transfers indicated that these were domestic wires and that the additional instructions did not cause funds to be transferred internationally, when in fact, they were being sent from a U.S. bank account to foreign bank accounts.

5. The Defendant Property constitutes proceeds of violations of 18 U.S.C. § 1343 (Wire Fraud) and is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

6. In sum, this is a case about clearing title to the Defendant Property, that is, monies swindled from victims through fraud and subsequently laundered, with the end goal of returning those monies to victims through the Department of Justice’s remission process.

#### **THE DEFENDANT IN REM**

7. The Defendant Property was seized on June 13, 2023, from MUFJ account ending in 0328, which is in the name of Bank 2, in the Southern District of New York. The Defendant Property is currently in the possession of the Finance and Accounting Division of Customs and Border Protection in New York, New York.

## **JURISDICTION AND VENUE**

8. This Court has subject matter jurisdiction over actions commenced by the United States under 28 U.S.C. § 1345, and over forfeiture actions under 28 U.S.C. § 1355(a) and (b).

9. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b)(1)(A) because the acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

10. Venue is proper within this judicial district under 28 U.S.C. § 1355(b)(1)(A) because the acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

## **FACTUAL ALLEGATIONS**

### **A. Investigation Background and Overview**

12. This Complaint involves criminal syndicates operating cryptocurrency investment and other fraud schemes. The scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S. victims. Scammers then fooled victims into “investing” in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal their money.

13. This type of scam involves scammers spending significant time getting to know and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds via wire transfer or through a provided

cryptocurrency deposit address. While the scammers prefer cryptocurrency deposits, they will also accept bank wires if the victim cannot transfer cryptocurrency.

14. As part of the scheme to defraud, the victims are told that they can expect to make a sizeable return on their investments. As investments are made, the spoofed websites falsely displayed a significant increase in the victim's account balance, which encouraged the victim to continue making investments. When the victim attempted to make a withdrawal, the scammers often attempted to coerce the victims to send even more funds. These tactics included requesting additional deposits due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempted to solicit additional investments from the victims, the victims were unable to recover their investment.

15. As of the filing of this Complaint, there are hundreds of victim transactions associated with this scam syndicate that operates primarily through the use of spoofed domains and is responsible for more than \$80 million directly traceable to reported victim losses. The "Identified Victim Transactions" columns in attached exhibits 1 and 2 represent transactions from shell companies to the Subject Account throughout the time period specified in each exhibit. Exhibit 1 covers a broader timeframe during which the scam operated, whereas exhibit 2 covers those transactions from which the \$13,475,175.67 Defendant Property is derived.

16. Once it obtained the victims' funds, the syndicate utilized various money laundering techniques to conceal the nature, source, and origin of the victim funds. These techniques included the use of money couriers, commercially unnecessary numbers of financial transactions, pooling of victim monies, and shell accounts.

B. Cryptocurrency Investment Scheme

17. The United States Secret Service (“USSS”) learned that a number of victims had been directed to invest at the spoofed domain simexlua.com. On or about September 1, 2022, USSS conducted an undercover operation in which an undercover agent (“UCA”) visited and created an account at this domain. The UCA began communicating with online customer service, through the website’s chat portal, about making investments. Shortly thereafter, online customer service provided the UCA with instructions to invest funds by sending a wire to a bank account in the name of a company named “Sea Dragon Remodel Inc.”

18. The bank account provided to the UCA was a JPMorgan Chase (“JPMC”) account ending in 5581 (“JPMC account 5581”). This account was opened by Hailong Zhu (“Zhu”) on October 21, 2022, for a business called Sea Dragon Remodel Inc. Zhu was the sole signatory listed on the account. In the documents used to open the bank account, Zhu provided an address on District Blvd in Vernon, California, along with other information.

19. Zhu was also the sole signatory of a JPMC bank account ending in 3886 (“JPMC account 3886”), which was opened as a business checking account on September 9, 2022, for a business called Sea Dragon Trading LLC. In the documents used to open the bank account, Zhu provided an address located on S El Molino St in Alhambra, California. Zhu opened a number of accounts in the names of these two Sea Dragon entities.

20. Zhu’s various bank accounts received wires from multiple confirmed scam victims. Included among those victims is an individual living in Falls Church, Virginia (“Victim 1”). At all times relevant to this Complaint, Victim 1 resided within the Eastern District of Virginia.

C. Victim Fund Transfers to Zhu’s Sea Dragon Accounts

21. In or around June of 2022, Victim 1 received an unsolicited phone contact from a woman identifying herself as “Rachel.” After many weeks of communication, “Rachel” introduced Victim 1 to a fraudulent cryptocurrency investment platform and encouraged him to “invest.” Victim 1 was directed to the spoofed domain coinasx.com, from where he was directed to download an application to his mobile device. The downloaded platform used the name “ASX,” which mimicked the Australian Securities Exchange. Victim 1 spoke with a purported customer service representative on the “coinasx.com” online chat portal, who explained to Victim 1 how to invest.

22. On or about August 12, 2022, and after Victim 1 was provided with wire instructions from an “ASX” online customer service representative, Victim 1 made a \$1,100 investment from his bank account in the Eastern District of Virginia. Victim 1 then began seeing significant “profits” in his account and invested additional money via at least six other wire transfers between August and at least November 2022. Victim 1 initiated these wires from within the Eastern District of Virginia.

23. “ASX” customer service provided Victim 1 with different accounts to which to send each wire transaction. On November 25, 2022, Victim 1 invested \$5,000 via a wire to Bank of America (“BOA”) account 9529 belonging to Sea Dragon Remodel Inc., for which Zhu was the sole signatory. Victim 1 also sent wires to accounts in the name of entities including Hights Kim Trading Inc (\$1,100 on August 12, 2022), PBB International Consulting (\$15,100 on September 2022), and Jishun Limited (\$5,000 on November 17, 2022). Victim 1 has been unable to make any withdrawals or recover any amount of his investments.

24. None of the entities to which Victim 1 transferred money had names with any relation to “ASX,” coinasx, or any other cryptocurrency investment site. Additionally, Hights

Kim Trading Inc, PBB International Consulting, and Jishun Limited have received funds from other fraud victims. Like Zhu's Sea Dragon entities, these other companies were shell companies incorporated to launder scam proceeds.

25. There are at least six other victims who have transferred money into either Zhu's BOA account 9529 or his JPMC account 3886.

D. Sea Dragon Account Funds Traceable to and through Subject Account

26. BOA account 9529 belonging to Sea Dragon Remodel Inc. received Victim 1's \$5,000 deposit on November 25, 2022. On November 29, 2022, \$53,000 was wired from BOA account 9529 to the Subject Account.<sup>1</sup>

27. The instructions affecting that wire to the Subject Account reveal the wire was initially sent to an MUFJ account ending 7694, which was Bank 1's correspondent account at MUFJ.

28. The instructions next included additional directions reading "For Further Credit to" the Subject Account. The "for further credit" instruction, sometimes written as "FFC," means that the proceeds should be "further credited"—*i.e.*, transferred—from account 7694 to the Subject Account.

29. There were eight total transactions from November to December 2022 totaling \$384,600 from Zhu's BOA account 9529 first to Bank 1's account 7694 and then to the Subject Account. At least seven other cryptocurrency investment fraud scam victims had also transferred money into BOA account 9529.

---

<sup>1</sup> In addition to Sea Dragon Remodel Inc., PBB International Consulting also received funds from Victim 1, and also transferred funds to the Subject Account.

30. Zhu's JPMC account 3886 engaged in similar transactions. For example, on October 12, 2022, JPMC account 3886 received \$31,000 from an individual who informed law enforcement that they were a victim of a cryptocurrency investment fraud scheme. On October 17, 2022, Zhu or other co-conspirators wired \$40,000 from JPMC account 3886 to the Subject Account. JPMC wire forms indicate that the initial recipient of this wire was again Bank 1's account 7694 at MUFJ. The wire instructions then directed that the money be further transferred to the Subject Account. Finally, the additional instructions state "Ffc 1002179 00 Axis Digital Limited." These additional instructions meant the funds were ultimately to be transferred to a Bank 2 customer named Axis Digital Limited.

31. Additionally, Zhu or other co-conspirators falsely indicated that this transfer was a domestic wire. By using this system of "for further credit" instructions, Zhu and his co-conspirators sent money abroad without being subject to the enhanced scrutiny that normally accompanies international transfers.

32. Numerous other transactions out of Zhu's Sea Dragon accounts were first routed to Bank 1 account 7694, then to the Subject Account, and then to Bank 2 account number 1001924, which is held by an entity named "GTAL." These transactions were similarly marked as domestic wires, despite ending abroad.

E. Investigation of Sea Dragon and Related Entities

33. Sea Dragon Trading and Sea Dragon Remodel were not legitimate businesses. Sea Dragon Trading was incorporated with the stated purpose of "general TRADING," and Sea Dragon Remodel was incorporated for "remodel and distribution of construction material." Associated bank records show no transactions that appeared to be related to "trading" or "remodel and distribution of construction material," such as incoming or outgoing payments to

or from construction suppliers or other trading businesses. Additionally, these businesses had no online presence and searches in the California Database of licensed contractors for Sea Dragon Remodel, Sea Dragon Trading, and Zhu, found no results.

34. Furthermore, the Sea Dragon bank accounts received mostly round number wires (*e.g.*, \$100,000 or \$75,000) coming in from remitters throughout the United States, including Massachusetts, Florida, Maryland, Illinois, Rhode Island, Kansas, Connecticut, New Jersey, Pennsylvania, South Dakota, Nebraska, Montana, and Louisiana, as well as one from Canada. It is inconsistent with being a “remodeling” or “trading” company based in California to receive wires from customers out of state, particularly from so many different states. It is also inconsistent for such a business account to receive so many transfers in round numbers, which do not reflect the typical cost variables associated with legitimate transactions for supplies, taxes, and services rendered in remodeling or “trade” businesses.

35. Zhu was arrested on March 21, 2023, based on his involvement in the scheme. Zhu’s role was to create entities, open business accounts, and execute wire transfers. Zhu was supervised in his role in the scam by Joseph Wong, among others. Zhu did not provide any services for the businesses he created (*i.e.*, he did not engage in construction or activities).

36. Joseph Wong played a supervisory role in the fraudulent scheme. Also on March 21, 2023, USSS agents executed search warrants at Wong’s residence, located in Rosemead, California. Pursuant to the search warrants, USSS agents seized numerous iPhone mobile devices belonging to Wong. Wong used at least three of these devices to conduct banking activity on behalf of others, including directing wire transfers in the names of different people, including Zhu. Agents also seized check stock, credit cards, and bank statements related to Sea Dragon Trading LLC, Sea Dragon Remodel Inc, Good Luck Trading LLC, Mingxing Trading LLC,

Mingxing Remodel LLC, and Hong's Trading LLC, among others. Between October 2022 to December 2022, each of the aforementioned shell companies received fraud proceeds and then subsequently wired such proceeds to the Subject Account, as depicted in exhibits 1 and 2.

37. For example, a victim in North Hempstead, NY ("Victim 2") was fraudulently induced to invest \$230,000 via four wires into a cryptocurrency investment platform later determined to be fraudulent. One of these wires was for \$25,000 on October 27, 2022, to Mingxing Trading, LLC's JPMC account ending 5251. On November 9, 2022, \$200,000 was transferred from this account to the Subject Account via Bank 1's correspondent account at MUFJ. The wire included the instructions "for further credit to" the Subject Account, with additional instructions "FFC" to GTAL.

F. Analysis of the Subject Account and Identification of Funds Subject to Forfeiture

38. The Subject Account is owned by Bank 2, a bank licensed and operating abroad. Bank 2 opened the Subject Account in or around September 2021.

39. In conducting a review of the Subject Account, MUFJ noted a high volume of wires that initially went to the Bank 1 correspondent account ending in 7694 and then contained additional instructions to forward the money to Axis Digital Limited or GTAL—the same transaction patterns outlined above. MUFJ flagged these transactions because the source of funds was unknown and an economic business purpose could not be determined. Additionally, MUFJ conducted open-source research on some of the companies originating the transactions and concluded they appeared to be shell companies.

40. There were approximately 224 wire transfers from June 2022 to March 2023 into the Subject Account that contained clear instructions directing them to be transferred to Axis Digital Limited or GTAL, totaling approximately \$29.5 million.

41. Aside from the aforementioned 224 wire transfers, an additional 253 wire transfers totaling approximately \$29 million fit the same pattern associated with the fraud and laundering scheme described above. These 253 wire transfers originated from the same account numbers, business entities, and/or business addresses as the wires where the visible instructions directed the funds to either Axis Digital or GTAL. The combination of the 224 wire transfers plus the 253 additional wire transfers discussed total \$58,465,480 from June 18, 2022, to March 2023.

42. Attached exhibit 1 lists the entities tied to fraudulent schemes that transferred this \$58,465,480 into the Subject Account with directions to further transfer money to Axis Digital or GTAL.<sup>2</sup> These entities and their bank accounts demonstrated similar patterns as the Sea Dragon entities discussed above, including round-number transfers and transaction activity that did not match the stated business purpose of the entity.

43. Of the 447 wires totaling \$58,465,480 from June 18, 2022, to March 2023, a sum of \$24,942,361 was invested in a Treasury Bill with CUSIP 912796CW7 on April 12, 2023.<sup>3</sup> Each purchase of CUSIP 912796CW7 represents an increase in the overall holding of that same Treasury Bill. This \$24,942,361 investment was one of fifteen purchases of this CUSIP between January 2023 and April 2023, totaling \$385,399,417. This \$24,942,361 consisted of wire fraud proceeds from the cryptocurrency investment fraud scheme alleged herein, most of which was

---

<sup>2</sup> The majority of these schemes were cryptocurrency investment fraud scams using spoofed cryptocurrency websites, as described above. Approximately ten additional victims had fallen prey to tech scams and fake order scams, and the proceeds for these scams were being laundered through the same shell companies and accounts. “Tech scams” relate to scammers posing as tech support such as “Geek Squad” and “MacAfee.” These scammers induce victim payments by making them believe they paid for a subscription or required tech services. “Fake order scams” relate to when scammers make victims believe they are receiving proceeds from sales. These “proceeds” are fictitious, and the scammer will induce the victim to wire a portion of these “proceeds” back to the scammer.

<sup>3</sup> A CUSIP number is a unique nine-digit identification number assigned to financial securities in the United States and Canada.

deposited into the Subject Account in February and March 2023. This purchase of the Treasury Bill had a face value of \$25,000,000 and was also held in the Subject Account.

44. On May 2, 2023, the same Treasury Bill with CUSIP 912796CW7 matured, and the full face value of the Treasury Bill was deposited into the cash side of the Subject Account. Given the fifteen total purchases of this CUSIP from January 2023 to April 2023, the full maturity value of the CUSIP was \$386,005,000. Even without accounting for appreciation, \$24,942,361 of that \$386,005,000 constituted wire fraud proceeds from the cryptocurrency investment fraud scheme described herein. Between May 2, 2023, and June 12, 2023, the lowest balance the cash side of the Subject Account reached was \$13,475,175.67. On June 13, 2023, this \$13,475,175.67, representing the proceeds from the cryptocurrency investment fraud scheme and the Defendant Property, was seized from the Subject Account pursuant to a seizure warrant issued by a U.S. Magistrate Judge.

**CLAIM FOR RELIEF**  
**(Forfeiture under 18 U.S.C. § 981(a)(1)(C)—Wire Fraud)**

45. The United States incorporates by reference paragraphs 1 through 44 above as if fully set forth herein.

46. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture “[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting ‘specified unlawful activity’ (as defined in section 1956(c)(7) of this title) or a conspiracy to commit such an offense.”

47. Title 18, United States Code, Section 1343 imposes a criminal penalty on any person who:

having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television

communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice...

48. Title 18, United States Code, Section 1349 imposes a criminal penalty on any person who conspires to commit wire fraud as set forth in 18 U.S.C. § 1343.

49. Title 18, United States Code, Section 2(a) provides that whoever aids, abets, counsels, commands, induces or procures the commission of an offense against the United States is punishable as a principal.

50. Title 18, United States Code, Section 1956(c)(7)(A) provides that the term “specified unlawful activity” includes “any act or activity constituting an offense listed in section 1961(1) of this title.” Title 18, United States Code, Section 1961(1) lists “any act which is indictable under any of the following provisions of title 18, United States Code. . . section 1343 (relating to wire fraud).”

51. As set forth above, the Defendant Property constitutes criminal proceeds of wire fraud, conspiracy to commit wire fraud, and aiding and abetting in wire fraud, in violation of 18 U.S.C. § 1343, 18 U.S.C. § 1349, and 18 U.S.C. § 2.

52. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

#### **PRAYER FOR RELIEF**

WHEREFORE, plaintiff requests that judgment be entered in its favor against the Defendant Property; that pursuant to law, notice be provided to all interested parties to appear and show cause why the forfeiture should not be decreed; that the Defendant Property be forfeited to the United States of America and delivered into its custody for disposition according to law; that plaintiff be awarded its costs and disbursements in this action; and for such and further relief as this Court may deem just and proper.

Dated: December 20, 2024

Respectfully submitted,

Jessica D. Aber  
United States Attorney

By: /s/ Kevin Hudson  
Kevin Hudson  
Assistant United States Attorney  
Virginia State Bar No. 81420  
Attorney for the United States  
11815 Fountain Way, Suite 200  
Newport News, Virginia 23606  
Office Number: (757) 591-4000  
Facsimile Number: (757) 591-0866  
Email Address: kevin.hudson@usdoj.gov

/s/  
Zoe Bedell  
Assistant United States Attorney  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
Office Number: (703) 299-3700  
Facsimile Number: (703) 299-3982  
Email Address: zoe.bedell@usdoj.gov

**VERIFICATION**

I, Teresa Healy, Special Agent, United States Secret Service, declare under penalty of perjury as provided by 28 U.S.C. § 1746, that the foregoing Complaint for Forfeiture in Rem is based on information known by me personally and/or furnished to me by various federal, state, and local law enforcement agencies, and that everything contained herein is true and correct to the best of my knowledge.

Executed at Los Angeles, California, this 20th of December, 2024.

  
\_\_\_\_\_  
Teresa Healy  
Special Agent  
United States Secret Service